

What is claimed are:

1. A door access control and key management system for a plurality of doors and a plurality of door users, the system comprising:

(a) a communications network;

5 (b) a door/key administering system for storing a key unique to each of the users, for storing an identification code unique to each of the doors, and for assigning access authorization to at least one user for each door, the door/key administering system being communicatively connected to the communications network; and

10 (c) a door lock/control assembly mounted on each door for reading the key presented by the user, for verifying that the key has access authorization, and for operating the door in response to the authorization for access, the door lock/control assembly being communicatively connected to the door/key administering system via the communications network;

15 (d) whereby a user can gain access to the doors authorized to the user with a unique key.

2. The system as claimed in claim 1, wherein the access given to a particular key to a particular door is communicated to the door/key administrator by the door control/lock assembly.

20 3. The system as claimed in claim 1, wherein the door control/lock assembly reads the key presented by a user and sends the read to the door/key administering system to obtain access authorization.

25 4. The system as claimed in claim 1, wherein the door control/lock assembly carries out the authorization process when the communication between the door assembly and the door/key administering system is interrupted.

5. The system as claimed in claim 1, wherein the communications network includes a wireless communications network.

6. The system as claimed in claim 1, wherein the communications network includes an IP (Internet Protocol) communications network, and the door/key administering system includes a door/key administering server system.

7. The system as claimed in claim 6, wherein the door control/lock assembly and the door/key administering server system are adapted to be controlled via a web browser operatively connected to the IP communications network.

8. The system as claimed in claim 1, wherein the key includes a key signature unique to the respective user and recognizable by the door control/lock assembly, the key signature being a numeric code, a sequence of numbers, a unique signal, or a biometric recognition code.

9. The system as claimed in claim 1, wherein the communication and authorization process between the door/key administering system and the door control/lock assembly are carried out in a form of encrypted signals or messages.

10. The system as claimed in claim 1, wherein each door control/lock assembly includes;

- (a) an identification device for reading the key presented by the users;
- (b) a lock adapted to be operated in response to the authorization from the door/key administering system; and
- (c) an embedded controller for controlling the operation of the identification device and the lock, and the authorization process.

11. The system as claimed in claim 10, wherein the door control/lock assembly includes two or more identification devices which are different from each other, and each user is assigned two or more different keys which corresponds to the two or more identification devices respectively, wherein each user can be authorized for access by using anyone of the different keys.

12. The system as claimed in claim 10, wherein the door control/lock assembly includes two or more identification devices which are different from each other, and each user is assigned two or more different keys which corresponds to the two or more identification devices respectively, wherein each user can be authorized for access by using all or several of the different keys.

13. The system as claimed in claim 10, wherein the door assembly is connected wirelessly to the communications network, and the door control/lock assembly further includes a wireless transmitter/receiver.

14. The system as claimed in claim 10, wherein the door control/lock assembly further includes means for assisting in the operation of the assembly and sensing the status of the assembly, the means including one or more of the following: a door open sensor, a speaker and microphone assembly, a camera, an activity light, a buzzer, a call button, a battery condition sensor, a smoke sensor, a temperature sensor.

15. The system as claimed in claim 10, wherein the embedded controller includes a database for storing information on the keys and users such that, when the communication between the door assembly and the door/key administering system is interrupted, the door control/lock assembly can carry out the authorization process for the door associated therewith.

16. The system as claimed in claim 10, wherein the key includes a key signature unique to the respective users and readable by the identification device,

the key signature including a numeric code, a sequence of numbers, a unique signal, or a biometric recognition code.

17. The system as claimed in claim 1, wherein the key/door administering system is physically separated into a key administering system and a door
5 administering system.

18. The system as claimed in claim 1, wherein the stored data pertaining to the keys and the doors can be updated when required.

19. The system as claimed in claim 1, wherein the door control/lock assembly and the door/key administering server system are adapted to be controlled by a web browser operatively connected to the communications network.
10

20. A method of controlling access to a plurality of doors by a plurality of door users via a communications network, the method comprising steps of:

(a) storing a unique identification code for each of the doors in a server;
(b) storing a unique key signature for each of the users in the server;
(c) assigning to each door the unique keys having access authorization to
15 the respective doors;

(d) comparing a user's key detected at the door to the keys having access authorization to the door in the server;

(e) authorizing access to the door; and

20 (f) wherein the authorization step is carried out through the communications network between the door and the server and each user can gain access to the doors authorized to the user with a unique key and each door can provide access to the user or users assigned thereto.

21. The method as claimed in claim 20, further comprising a step of
25 storing two or more different unique key signatures for the user whereby all of the different key signatures are required to gain access to the door.

22. The method as claimed in claim 21, wherein any one of the different key signatures is required to gain access to the door.

23. The method as claimed in claim 20, wherein the communications networks includes an IP communications networks.

5 24. The method as claimed in claim 20, wherein the communications networks includes a wireless communications networks.

25. A system architecture for controlling a plurality of door access control and key management systems, the system architecture comprising:

10 (a) the plurality of door access control and key management systems according to claim 1, the systems being communicatively and operatively connected to a communication network; and

15 (b) a Meta server being adapted to serve as an address reference among the door access control and key management systems, the Meta server being communicatively and operatively connected to each of the door access control and key management systems via the communications network, wherein the Meta server contains the address of each door access control and key management system and its associated unique key ID codes and unique door ID codes and each door access control and key management system contains the address of the Meta server.

20 26. The system architecture as claimed in claim 25, wherein the communications network includes an IP communications network.

27. The system architecture as claimed in claim 25, wherein the Meta server is adapted to be controlled via a web browser communicatively and operatively connected to the Meta server through the communications network.